UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE: GOOGLE INC. GMAIL LITIGATION THIS DOCUMENT RELATES TO: **ALL ACTIONS**	Case No.: 13-MD-02430-LHK ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO DISMISS [REDACTED]

In this consolidated multi-district litigation, Plaintiffs Keith Dunbar, Brad Scott, Todd Harrington, Matthew Knowles, A.K. (next of friend to Minor J.K.), Brent Matthew Scott, Kristen Brinkman, Robert Fread, and Rafael Carrillo, individually and on behalf of those similarly situated (collectively, "Plaintiffs"), allege that Defendant Google, Inc., has violated state and federal anti-wiretapping laws in its operation of Gmail, an email service. *See* ECF No. 38-2. Before the Court is Google's Motion to Dismiss Plaintiffs' Consolidated Complaint. *See* ECF No. 44. For the reasons stated below, the Court DENIES in part and GRANTS in part Google's Motion to Dismiss with leave to amend.

I. BACKGROUND

A. Factual Allegations

Plaintiffs challenge Google's operation of Gmail under state and federal anti-wiretapping laws. The Consolidated Complaint seeks damages on behalf of a number of classes of Gmail users and non-Gmail users for Google's interception of emails over a period of several years. All the class periods span from two years prior to the filing of the actions to the date of class certification, if any. Because the first of these consolidated actions was filed in 2010, the Consolidated Complaint taken as a whole challenges the operation of Gmail from 2008 to the present.

1. Google's Processing of Emails

Google's processing of emails to and from its users has evolved over the putative class periods. Plaintiffs allege, however, that in all iterations of Google's email routing processes since 2008, Google has intercepted, read, and acquired the content of emails that were sent or received by Gmail users while the emails were in transit. Plaintiffs allege that before [redacted] 20[redacted], a Gmail device intercepted, read, and acquired the content of each email for the purposes of sending an advertisement relevant to that email communication to the recipient, sender, or both. ECF No. 38-2 ¶¶ 26–27, 33. According to the Consolidated Complaint, this interception and reading of the email was separate from Google's other processes, including spam and virus filtering. *Id.* ¶ 5.

After [redacted] 20[redacted], Plaintiffs allege that Google continued to intercept, read, and acquire content from emails that were in transit even as Google changed the way it transmits emails. Plaintiffs allege that after [redacted] 20[redacted], Google continued to intercept, read, and acquire content from emails to provide targeted advertising. *Id.* ¶¶ 62–63. Moreover, Plaintiffs allege that post-[redacted] 20[redacted], targeted advertising was not the sole purpose of the interception. Rather, during this time period, Plaintiffs allege that a number of Google devices intercepted the emails, read and collected content as well as affiliated data, and [redacted] these emails and data. *Id.* ¶¶ 47–56. Plaintiffs further allege that Google used these [redacted] data to create user profiles and models. *Id.* ¶¶ 74–79. Google then allegedly used the emails, affiliated data, and user profiles to serve their

profit interests that were unrelated to providing email services to particular users. *Id.* ¶¶ 97–98. Accordingly, Plaintiffs allege that Google has, since 20[redacted], intercepted emails for the dual purposes of providing advertisements and creating user profiles to advance Google's profit interests.

2. Types of Gmail Services

Gmail implicates several different, but related, systems of email delivery, three of which are at issue here. The first is a free service, which allows any user to register for an account with Google to use Gmail. *Id.* ¶ 99. This system is supported by advertisements, though users can opt-out of such advertising or access Gmail accounts in ways that do not generate advertising, such as accessing email on a smartphone. *Id.* ¶ 70.

The second is Google's operation of email on behalf of Internet Service Providers ("ISPs"). *Id.* ¶ 100. Google, through its Google Apps Partner program, enters into contracts with ISPs, such as Cable One, to provide an email service branded by the ISP. *Id.* The ISP's customers can register for email addresses from their ISP (such as "@mycableone.com"), but their email is nevertheless powered by Google through Gmail.

Third, Google operates Google Apps for Education, through which Google provides email on behalf of educational organizations for students, faculty, staff, and alumni. *Id.* ¶ 101. These users receive "@name.institution.edu" email addresses, but their accounts are also powered by Google using Gmail. *Id.* Universities that are part of Google Apps for Education require their students to use the Gmail-provided service. *Id.*

Google Apps users, whether through the educational program or the partner program, do not receive content-based ads but can opt in to receiving such advertising. Google processes emails sent and received from all Gmail users,[1] including Google Apps users, in the same way

[1] In this Order, the Court uses "Gmail users" to refer to individuals who send or receive emails using the free Gmail service or Google apps. "Non-Gmail users" refers to email users who do not themselves use Gmail (through the free service or Google Apps). "Google Apps users" refers to the subset of Gmail users who access Gmail through either the Google Apps Partner Program or Google Apps for Education.

except that emails of users who do not receive advertisements are not processed through Google's advertising infrastructure, which attaches targeted advertisements to emails. *Id.* ¶¶ 57, 72–73. This means that users who do not receive advertisements would not have been subject to the pre-[redacted] 20[redacted] interceptions, as during that period, interceptions were for the sole purpose of attaching targeted advertisements to emails. After [redacted] 20[redacted], Google separated its interception of emails for targeted advertising from its interception of emails for creating user profiles. *Id.* ¶ 72. As a result, after [redacted] 20[redacted], emails to and from users who did not receive advertisements are nevertheless intercepted to create user profiles. *Id.* ¶¶ 73, 85. Accordingly, these post-[redacted] 20[redacted] interceptions impacted all Gmail and Google Apps users, regardless of whether they received advertisements.

3. Google's Agreements with Users

The operation of the Gmail service implicates several legal agreements. Gmail users were required to agree to one of two sets of Terms of Service during the class periods. The first Terms of Service was in effect from April 16, 2007, to March 1, 2012, and the second has been in effect since March 1, 2012. *Id.* ¶ 102. The 2007 Terms of Service stated that:

> Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service. For some Services, Google may provide tools to filter out explicit sexual content. These tools include the SafeSearch preference settings . . . . In addition, there are commercially available services and software to limit access to material that you may find objectionable.

Id. ¶ 104. A subsequent section of the 2007 Terms of Service provided that "[s]ome of the Services are supported by advertising revenue and may display advertisements and promotions" and that "[t]hese advertisements may be content-based to the content information stored on the Services, queries made through the Service or other information." *Id.* ¶¶ 107–08.

The 2012 Terms of Service deleted the above language and stated that users "give Google (and those [Google] work[s] with) a worldwide license to use . . ., create derivative works (such as

those resulting from translations, adaptations or other changes we make so that your content works better with our Services), . . . and distribute such content." *See* ECF No. 46-6 at 3.

Both Terms of Service reference Google's Privacy Policies, which have been amended three times thus far during the putative class periods. *See* ECF Nos. 46-7, 46-8, 46-9, 46-10. These Policies, which were largely similar, stated that Google could collect information that users provided to Google, cookies, log information, user communications to Google, information that users provide to affiliated sites, and the links that a user follows. *See* ECF No. 46-7. The Policies listed Google's provision of "services to users, including the display of customized content and advertising" as one of the reasons for the collection of this information. *Id.*

Google also had in place Legal Notices, which stated that "Google does not claim any ownership in any of the content, including any text, data, information, images, photographs, music, sound, video, or other material, that [users] upload, transmit or store in [their] Gmail account." ECF No. 38-2 ¶ 118. The Notices further stated that Google "will not use any of [users'] content for any purpose except to provide [users] with the service." *Id.* ¶ 121.

In addition, Google entered into contractual agreements with ISPs and educational institutions as part of its Google Apps Partner and Google Apps for Education programs. These agreements require Google to "protect against unauthorized access to or use of Customer data." *Id.* ¶¶ 137, 161. In turn, "Customer data" is defined as "data, including email, provided, generated, transmitted, or displayed via the Services by Customers or End Users." *Id.* ¶¶ 138, 162. Further, the Terms of Service applicable to Google Apps Cable One users states that "Google may access, preserve, and disclose your account information and any Content associated with that account if required to do so by law or in a good faith belief that such access preservation or disclosure is reasonably necessary" to satisfy applicable law, enforce the Terms of Service, detect or prevent fraud, or protect against imminent harm to the rights of Google, its users, or the public. ECF No. 46-2 at 2–3.

Importantly, Plaintiffs who are not Gmail or Google Apps users are not subject to any of Google's express agreements. Because non-Gmail users exchange emails with Gmail users, however, their communications are nevertheless subject to the alleged interceptions at issue in this case.

4. Relief Sought and Class Allegations

Plaintiffs bring these cases alleging that Google, in the operation of its Gmail system, violated federal and state anti-wiretapping laws. ECF No. 38-2 ¶ 216 (federal law), ¶ 288 (California law), ¶ 328 (Maryland law), ¶ 349 (Florida law), ¶ 370 (Pennsylvania law). Plaintiffs seek the certification of several classes, preliminary and permanent injunctive relief, declaratory relief, statutory damages, punitive damages, and attorneys' fees. Plaintiffs seek relief on behalf of the following classes, all of which have a class period starting two years before the relevant complaint was filed and running through the date of class certification, if any:

(1) all Cable One users who sent a message to a Gmail user and received a reply or received an email;

(2) all Google Apps for Education users who have sent a message to a Gmail user and received a reply or received an email;

(3) all U.S. citizen non-Gmail users (except California residents) who have sent a message to a Gmail user and received a reply or received an email from a Gmail user;

(4) all U.S. citizen non-Gmail users who have sent a message to a Gmail user and received a reply or received an email from a Gmail user;

(5) all Pennsylvania non-Gmail users who have sent a message to a Gmail user and received a reply or received an email from a Gmail user;

(6) all Florida non-Gmail users who have sent a message to a Gmail user and received a reply or received an email from a Gmail user;

(7) all Maryland non-Gmail users who have sent a message to a Gmail user and received a reply or received an email from a Gmail user; and

(8) all Gmail users who were under the age of majority and who used Gmail to send an email to or received an email from a non-Gmail user or a Gmail user under the age of majority. *Id.* ¶¶ 388–92.

B. Procedural History

This case is a consolidated multi-district litigation involving seven individual and class action lawsuits. *See* ECF No. 38-2. The first of these consolidated actions was filed on November 17, 2010, and transferred from the Eastern District of Texas to the Northern District of California on June 27, 2012. *See Dunbar v. Google, Inc.*, 12-CV-03305 (N.D. Cal.); ECF No. 179. Five other actions involving substantially similar allegations against Google followed in this District and throughout the country. *See Scott, et al. v. Google, Inc.*, No. 12-CV-03413 (N.D. Cal.); *Scott v. Google, Inc.*, No. 12-CV-00614 (N.D. Fla.); *A.K. v. Google, Inc.*, No. 12-CV-01179 (S.D. Ill.); *Knowles v. Google, Inc.*, 12-CV-02022 (D. Md.); *Brinkman v. Google, Inc.*, 12-CV-06699 (E.D. Pa.). On April 1, 2013, the Judicial Panel on Multidistrict Litigation issued a Transfer Order, centralizing these six actions in the Northern District of California before the undersigned judge. *See* ECF No. 1. On May 6, 2013, this Court related a seventh action, *Fread v. Google, Inc.*, 13-CV-01961 (N.D. Cal.), as part of this multi-district litigation. *See* ECF No. 29.

Plaintiffs filed an Administrative Motion to file their Consolidated Complaint under seal on May 16, 2013.[2] *See* ECF No. 38. The Complaint contained five claims alleging violations of: (1) the Wiretap Act, as amended by the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510, *et seq.*; (2) the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630, *et seq.*; (3) the Maryland Courts and Judicial Proceedings Code Ann. §§ 10-402, *et seq.*; (4) Florida Statute §§ 934.03, *et seq.*; and (5) 18 Pa. Const. Stat. §§ 5701, *et seq.* *See* ECF No. 38-2.

Google filed a Motion to Dismiss the Consolidated Complaint on June 13, 2013. *See* ECF No. 44. On the same day, Google filed two declarations and a request for judicial notice in support

[2] The Court resolves this Administrative Motion through a separate order.

of its Motion. *See* ECF Nos. 45–47. Plaintiffs filed an opposition to Google's request for judicial notice and separate objections to Google's declarations on July 11, 2013. *See* ECF Nos. 49–50. Google filed a reply in support of its request for judicial notice and Motion to Strike Plaintiffs' objections to Google's declarations on July 29, 2013. ECF No. 58.

Plaintiffs filed their opposition to Google's Motion to Dismiss on July 11, 2013. *See* ECF No. 53. That same day, Plaintiffs filed a request for judicial notice in support of their opposition. *See* ECF No. 51. Google filed a reply along with a declaration in support of the reply on July 29, 2013. *See* ECF No. 56–57. This Court held a hearing on the Motion to Dismiss on September 5, 2013. *See* ECF No. 64.

II. LEGAL STANDARDS

A. Motion to Dismiss

Pursuant to Federal Rule of Civil Procedure 12(b)(6), a defendant may move to dismiss an action for failure to allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal citations omitted). For purposes of ruling on a Rule 12(b)(6) motion, the Court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the non-moving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

However, a court need not accept as true allegations contradicted by judicially noticeable facts, *Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and a "court may look beyond the plaintiff's complaint to matters of public record" without converting the Rule 12(b)(6) motion into a motion for summary judgment, *Shaw v. Hahn*, 56 F.3d 1128, 1129 n.1 (9th Cir. 1995). A court is also not required to "'assume the truth of legal conclusions merely because they are cast in

the form of factual allegations.'" *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per curiam) (quoting *W. Min. Council v. Watt*, 643 F.2d 618, 624 (9th Cir. 1981)). Mere "conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss." *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004); *accord Iqbal*, 556 U.S. at 678. Furthermore, "a plaintiff may plead herself out of court" if she "plead[s] facts which establish that [s]he cannot prevail on h[er] . . . claim." *Weisbuch v. Cnty. of L.A.*, 119 F.3d 778, 783 n.1 (9th Cir. 1997) (internal quotation marks and citation omitted).

B. Request for Judicial Notice

The Court generally may not look beyond the four corners of a complaint in ruling on a Rule 12(b)(6) motion, with the exception of documents incorporated into the complaint by reference, and any relevant matters subject to judicial notice. *See Swartz v. KPMG LLP*, 476 F.3d 756, 763 (9th Cir. 2007); *Lee v. City of Los Angeles*, 250 F.3d 668, 688–89 (9th Cir. 2001). Under the doctrine of incorporation by reference, the Court may consider on a Rule 12(b)(6) motion not only documents attached to the complaint, but also documents whose contents are alleged in the complaint, provided the complaint "necessarily relies" on the documents or contents thereof, the document's authenticity is uncontested, and the document's relevance is uncontested. *Coto Settlement v. Eisenberg*, 593 F.3d 1031, 1038 (9th Cir. 2010); *see Lee*, 250 F.3d at 688–89. The purpose of this rule is to "prevent plaintiffs from surviving a Rule 12(b)(6) motion by deliberately omitting documents upon which their claims are based." *Swartz*, 476 F.3d at 763 (internal quotation marks omitted).

The Court also may take judicial notice of matters that are either (1) generally known within the trial court's territorial jurisdiction or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. Fed. R. Evid. 201(b). Proper subjects of judicial notice when ruling on a motion to dismiss include legislative history reports, *see Anderson v. Holder*, 673 F.3d 1089, 1094, n.1 (9th Cir. 2012); court documents already in the public record and documents filed in other courts, *see Holder v. Holder*, 305 F.3d 854, 866 (9th

Cir. 2002); and publically accessible websites, *see Caldwell v. Caldwell*, 2006 WL 618511, at *4 (N.D. Cal. Mar. 13, 2006); *Wible v. Aetna Life Ins. Co.*, 375 F. Supp. 2d 956, 965–66 (C.D. Cal. 2005).

C. Leave to Amend

If the Court determines that the complaint should be dismissed, it must then decide whether to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend "shall be freely given when justice so requires," bearing in mind "the underlying purpose of Rule 15 . . . [is] to facilitate decision on the merits, rather than on the pleadings or technicalities." *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (internal quotation marks and citation omitted). Nonetheless, a court "may exercise its discretion to deny leave to amend due to 'undue delay, bad faith or dilatory motive on part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party . . ., [and] futility of amendment.'" *Carvalho v. Equifax Info. Servs., LLC*, 629 F.3d 876, 892–93 (9th Cir. 2010) (quoting *Foman v. Davis*, 371 U.S. 178, 182 (1962)) (alterations in original).

III. REQUESTS FOR JUDICIAL NOTICE

In support of their opposition to Google's Motion to Dismiss, Plaintiffs request the Court take judicial notice of (A) a declaration and a motion filed in *Sheppard v. Google, Inc., et al*, 12-CV-4022 (W.D. Ark.); (B) an excerpt of a November 30, 1985 Senate Judiciary Committee hearing regarding the ECPA; (C) an April 29, 1968 Senate Report; and (D) an order on Google's motion to dismiss in *Marquis v. Google, Inc.*, No. 11-2808, in the Superior Court of Suffolk County, Commonwealth of Massachusetts. *See* ECF No. 51. Plaintiffs' Exhibits B and C are legislative history reports, and Plaintiffs' Exhibits A and D are documents filed in other courts, already part of the public record. *See Anderson*, 673 F.3d at 1094, n.1; *Holder*, 305 F.3d at 866. Google does not oppose any of these requests. The Court takes judicial notice of all four.

Google requests that the Court take judicial notice of (A) a copy of Google's Terms of Service applicable to Google Apps services provided through Cable One, Inc.; (B) a copy of the

Google Apps Education Edition Agreement between Google and the University of Hawaii; (C) a copy of the Google Apps Education Edition Agreement between Google and the University of the Pacific; (D) copies of Google's Terms of Service dated April 16, 2007 and March 1, 2012; (E) copies of Google's Privacy Policies dated August 7, 2008, March 11, 2009, October 3, 2010, and March 1, 2012; (F) a copy of the Yahoo! Mail Privacy Policy from June 2013; (G) an excerpt of an October 17, 1986 Senate Report regarding the ECPA; (H) a copy of a May 9, 1995 California Senate Judiciary Committee analysis; and (I) a copy of an April 13, 2010 California Senate Public Safety Committee analysis. *See* ECF No. 47. Plaintiffs oppose the request for judicial notice with respect to items F, G, H, and I. *See* ECF No. 49.

The Court takes judicial notice of items A, B, C, D, and E as requested by Google and to which Plaintiffs do not object because Plaintiffs rely upon and reference these documents in the Complaint. *See* ECF No. 38-2 ¶¶ 102, 144, 185–86, 189, 227–28, 237–38; *Coto*, 593 F.3d at 1038. The Court further takes judicial notice of items H and I because Plaintiffs "do[] not contest that these are readily available public documents or challenge their authenticity." *Zephyr v. Saxon Mortg. Servs., Inc.*, 873 F. Supp. 2d 1223, 1226 (E.D. Cal. 2012). The Court takes judicial notice of item G because it is a legislative history report for the statute at the heart of Plaintiffs' principal claim. *See id.; Anderson*, 673 F.3d at 1094, n.1. Finally, the Court denies Google's request for judicial notice of item F, the Yahoo! Mail Privacy Policy. The Policy is not a document "on which the Complaint necessarily relies nor . . . whose relevance and authenticity are uncontested" because Plaintiffs contend that the effective dates of the Yahoo! Privacy Policy are unknown. *See* ECF No. 49 at 2–3; *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 795 (N.D. Cal. 2011).

Plaintiffs further raise objections to various paragraphs in the declarations supporting Google's Motion to Dismiss and to the requests for judicial notice with respect to some of the exhibits attached to the declarations. *See* ECF No. 50. The Court strikes these objections pursuant to Civil Local Rule 7-3(a). The Rule requires that any evidentiary objections to a motion be contained within the opposition to the motion itself, but Plaintiffs filed their objections separately

from their opposition. *See Apple, Inc. v. Samsung Elecs. Co., Ltd.*, 2011 WL 7036077, at *3 (N.D. Cal. Dec. 2, 2011).

IV. MOTION TO DISMISS

A. The Wiretap Act

The Wiretap Act, as amended by the ECPA, generally prohibits the interception of "wire, oral, or electronic communications." 18 U.S.C. § 2511(1); *see also Joffe v. Google, Inc.*, No. 11-17483, 2013 WL 4793247, at *3 (9th Cir. Sept. 10, 2013). More specifically, the Wiretap Act provides a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a); *see id.* § 2520 (providing a private right of action for violations of § 2511). The Act further defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4).

Plaintiffs contend that Google violated the Wiretap Act in its operation of the Gmail system by intentionally intercepting the content of emails that were in transit to create profiles of Gmail users and to provide targeted advertising. Google contends that Plaintiffs have not stated a claim with respect to the Wiretap Act for two reasons. First, Google contends that there was no interception because there was no "device." Specifically, Google argues that its reading of any emails would fall within the "ordinary course of business" exception to the definition of device. ECF No. 44 at 6–13. Under that exception, "any telephone or telegraph instrument, equipment or facility, or any component thereof . . . being used by a provider of wire or electronic communication service in the ordinary course of its business" is not a "device," and the use of such an instrument accordingly falls outside of the definition of "intercept." 18 U.S.C. § 2510(5)(a)(ii). Second, Google contends that all Plaintiffs have consented to any interception. ECF No. 44 at 13–20. Under the statute, it is not unlawful "to intercept a wire, oral, or electronic communication . . .

where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d).

1. "Ordinary Course of Business" Exception

Google first contends that it did not engage in an interception because its reading of users' emails occurred in the ordinary course of its business. ECF No. 44 at 6–13. Conversely, Plaintiffs contend that the ordinary course of business exception is narrow and applies only when an electronic communication service provider's actions are "necessary for the routing, termination, or management of the message." *See* ECF No. 53 at 7. The Court finds that the ordinary course of business exception is narrow. The exception offers protection from liability only where an electronic communication service provider's interception facilitates the transmission of the communication at issue or is incidental to the transmission of such communication. Specifically, the exception would apply here only if the alleged interceptions were an instrumental part of the transmission of email. Plaintiffs have alleged, however, that Google's interception is not an instrumental component of Google's operation of a functioning email system. ECF No. 38-2 ¶ 97. In fact, Google's alleged interception of email content is primarily used to create user profiles and to provide targeted advertising — neither of which is related to the transmission of emails. *See id.* ¶¶ 26–27, 33, 57, 65, 84, 95. The Court further finds that Plaintiffs' allegations that Google violated Google's own agreements and internal policies with regard to privacy also preclude application of the ordinary course of business exception.

The plain language of the Wiretap Act, 18 U.S.C. § 2510(5)(a), exempts from the definition of "device":

> any telephone or telegraph instrument, equipment or facility, or any component thereof,
>
> (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

> (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

This section includes two "ordinary course of business" exceptions. The first, under subsection (a)(i), is for users or subscribers of electronic communication services, while the second, subsection (a)(ii), applies to the providers of electronic communication services themselves. This case implicates the latter, as Google provides the electronic communication service at issue here, Gmail.

The Sixth Circuit has found that the text of "[t]he two exceptions [is] not altogether clear." *Adams v. City of Battle Creek*, 250 F.3d 980, 982 (6th Cir. 2001). There is no dispute that Google's interception of Plaintiffs' emails and subsequent use of the information to create user profiles or to provide targeted advertising advanced Google's business interests. But this does not end the inquiry. The Court must give effect to the word "ordinary," which limits "course of business" under both exceptions. The presence of the modifier "ordinary" must mean that not everything Google does in the course of its business would fall within the exception. The task the Court faces at this stage is to determine whether Plaintiffs have adequately alleged that the purported interceptions were not an "ordinary" part of Google's business.

In the context of section 2510(5)(a)(i), courts have held, consistent with the textual limitation that "ordinary" imposes on "course of business," that not everything that a company may want to do falls within the "ordinary course of business" exception. *See e.g., Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983) ("The phrase 'in the ordinary course of business' cannot be expanded to mean anything that interests a company."). Rather, the business reasons must be "legitimate." *See Arias v. Mut. Cent. Alarm Serv., Inc.*, 202 F.3d 553, 559 (2d Cir. 2000); *see also Berry v. Funk*, 146 F.3d 1003, 1009 (D.C. Cir. 1998) (finding that actions are in the ordinary course of business if they are "justified by a valid business purpose" or "shown to be undertaken normally").

This limitation, applied to electronic communication service providers in the context of section 2510(5)(a)(ii), means that the electronic communication service provider engaged in the alleged interception must demonstrate the interception facilitated the communication service or was incidental to the functioning of the provided communication service. For example, in *Kirch v. Embarq Management Co.*, 702 F.3d 1245 (10th Cir. 2012), which Google cites, ECF No. 44 at 9, the Tenth Circuit affirmed a grant of summary judgment in favor of Embarq, an ISP, where Embarq had intercepted only data incidental to its provision of the internet service. In that case, Embarq had granted a third party, NebuAd, permission to conduct a technology test by acquiring information about Embarq's users so that NebuAd could provide targeted advertising to those users. 702 F.3d at 1247. The Tenth Circuit held that Embarq had not violated the ECPA because the ISP could not be liable for NebuAd's interceptions. *Id.* at 1249. Further, Embarq itself did not review any of the raw data that NebuAd collected. *Id.* at 1250. Rather, Embarq had no more access than it otherwise would have had as an ISP. *Id.* Embarq's ordinary course of business as an ISP necessarily required that it would have access to data that was transmitted over its equipment. *Id.* at 1249. The relationship between Embarq and NebuAd's technology test did not expand the universe of data to which Embarq had access beyond the data Embarq could access in its provision of internet services. *Id.* at 1250. Accordingly, Embarq's actions fell within its ordinary course of business. Unlike this case, the only information to which Embarq had access was collected by Embarq's devices that provided internet services. *Id*. In contrast, here, Plaintiffs allege that there are separate devices — aside from the devices related to delivery of email — that intercept users' emails. ECF No. 38-2 ¶ 259(e). Considered practically, Google is more akin to NebuAd, which intercepted data for the purpose of providing targeted advertising — a purpose separate and apart from Embarq's provision of internet service. *Cf. Kirch*, 702 F.3d at 1248. However, because NebuAd settled with the Plaintiffs in *Kirch*, the Tenth Circuit's opinion does not deal with NebuAd's liability. *Id.* at 1248 n. 2, 1249 ("[W]e need not address whether NebuAd intercepted any of the Kirches' electronic communications."). The Court therefore finds that *Kirch*'s

discussion of Embarq's liability cuts in favor of a narrow reading of the section 2510(5)(a)(ii) exception and that *Kirch* stands only for the narrow proposition that interceptions incidental to the provision of the alleged interceptor's internet service fall within the "ordinary course of business" exception.

Hall v. Earthlink Network, Inc., 396 F.3d 500 (2d Cir. 2005), which also addresses the section 2510(5)(a)(ii) exception, further suggests that this Court should narrowly read the "ordinary course of business" exception. There, the Second Circuit affirmed a grant of summary judgment and concluded that Earthlink did not violate the ECPA when Earthlink continued to receive and store emails sent to an address that had been closed. The Second Circuit found that the plaintiff in that case did not present any evidence that Earthlink's continued receipt of emails was outside its ordinary course of business. *Id.* at 505. The Court noted that Earthlink presented testimony that Earthlink routinely continued to receive and store emails after an account was canceled and more critically that Earthlink "did not have the ability to bounce e-mail back to senders after the termination of an account." *Id.* Accordingly, in *Hall*, the email provider's alleged interceptions were a necessary part of its ability to provide email services. In the instant case, by contrast, Plaintiffs have alleged that Google could operate its Gmail system without reading the emails for the purposes of targeted advertising or the creation of user profiles. ECF No. 38-2 ¶ 97. Therefore, unlike *Earthlink*, the alleged interception in the instant case is not incidental to the operation of the service.[3]

[3] The Court finds that *In re Google, Inc. Privacy Policy Litigation*, 2012 WL 6738343 (N.D. Cal. Dec. 28, 2012), does not suggest a broader reading of the exception. Google relies on that case for the proposition that as long as Google is using its own devices, Google cannot be intercepting users' information. ECF No. 44 at 9–10. Yet, the court in *Privacy Policy* explicitly noted that the use of the device must be in the ordinary course of business. *See In re Google, Inc. Privacy Policy Litigation*, 2012 WL 6738343 at *5–6. Further, unlike that case, the alleged interception in the instant case occurred while the email was in transit, rather than when the material was already in possession of the intended recipient. *See id.* at *6 (dismissing plaintiffs' cause of action on the basis that they "utterly fail . . . to cite any authority that supports either the notion that a provider can intercept information already in its possession by violating limitations imposed by a privacy policy or the inescapably plain language of the Wiretap Act that excludes from the definition of a 'device' a provider's own equipment used in the ordinary course of business."). The difference

In addition to the text and the case law, the statutory scheme and legislative history also weigh in favor of a narrow reading of the section 2510(5)(a)(ii) exception. Specifically, a separate exception to the Wiretap Act related to electronic service providers states that:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring *except for mechanical or service quality control checks*.

18 U.S.C. § 2511(2)(a)(i) (emphasis added). The statute explicitly limits the use of service observing or random monitoring by electronic communication service providers to mechanical and service quality control checks. *Id.* Accordingly, the statutory scheme suggests that Congress did not intend to allow electronic communication service providers unlimited leeway to engage in any interception that would benefit their business models, as Google contends. In fact, this statutory provision would be superfluous if the ordinary course of business exception were as broad as Google suggests. *See Duncan v. Walker*, 533 U.S. 167, 174 (2001) (stating that in statutory interpretation, courts should "give effect, if possible, to every clause and word of a statute").

The legislative history of section 2511(2)(a)(i), which Google cites, ECF No. 44 at 7, also supports reading the ordinary course of business exception to require that the interception be instrumental to the provision of the service. A U.S. Senate Report regarding the ECPA states that "[t]he provider of electronic communications services may have to monitor a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain. These monitoring functions, which may be necessary to the provision of an electronic communication service, do not involve humans listening in on voice conversations. Accordingly, they are not prohibited." ECF No. 45-2 at 20. This suggests that Congress intended

---

between communications stored in the recipient's possession and those in transit is significant for the purposes of the statutory scheme as discussed *infra*.

to protect electronic communication service providers from liability when the providers were monitoring communications for the purposes of ensuring that the providers could appropriately route, terminate, and manage messages. Accordingly, the Court concludes that the legislative history supports a narrow reading of the section 2510(5)(a)(ii) exception, under which an electronic communication service provider must show some link between the alleged interceptions at issue and its ability to operate the communication system. Google's broader reading of the exception would conflict with Congressional intent.

The case law applying the "ordinary course of business" exception in the 2510(5)(a)(i) context also suggests that courts have narrowly construed that phrase. For example, in *Arias v. Mutual Central Alarm Service, Inc.*, the Second Circuit found that it was within an alarm company's ordinary course of business to record all incoming and outgoing calls because maintaining records of the calls was instrumental "to ensure that [the alarm company's] personnel are not divulging sensitive customer information, that events are reported quickly to emergency services, that customer claims regarding events are verifiable, and that the police and other authorities may rely on these records in conducting any investigations." 202 F.3d at 559 (internal quotation marks and alterations omitted). Similarly, the Tenth Circuit found that an employer's installation of a telephone monitoring device on the phone lines in departments where employees interacted with the public was within the employer's ordinary course of business because of "concern by management over abusive language used by irate customers when called upon to pay their bills, coupled with the possible need to give further training and supervision to employees dealing with the public." *James v. Newspaper Agency Corp.*, 591 F.2d 579, 581 (10th Cir. 1979).

The narrow construction of "ordinary course of business" is most evident in section 2510(5)(a)(i) cases where an employer has listened in on employees' phone calls in the workplace. *See United States v. Murdock*, 63 F.3d 1391, 1396 (6th Cir. 1995) (noting that "[a] substantial body of law has developed on the subject of ordinary course of business in the employment field where employees have sued their employers" and that "[t]hese cases have narrowly construed the phrase

'ordinary course of business'"); *Watkins*, 704 F.2d at 582. These cases suggest that an employer's eavesdropping on an employee's phone call is only permissible where the employer has given notice to the employee. *See Adams*, 250 F.3d at 984 (finding that the exception generally requires that the use be "(1) for a legitimate business purpose, (2) routine, and (3) with notice"). Further, these cases have suggested that an employer may only listen to an employee's phone call for the narrow purpose of determining whether a call is for personal or business purposes. In *Watkins*, for example, the court held that an employer "was obliged to cease listening as soon as she had determined that the call was personal, regardless of the contents of the legitimately heard conversation." 704 F.2d at 584. *Watkins* concerned a situation in which an employer listened in on an employee's personal phone call wherein the employee discussed a job interview. The Eleventh Circuit reversed a grant of summary judgment in favor of the employer notwithstanding the fact that the interception concerned a conversation that was "obviously of interest to the employer." *Id.* at 583–84.

These cases suggest a narrow reading of "ordinary course of business" under which there must be some nexus between the need to engage in the alleged interception and the subscriber's ultimate business, that is, the ability to provide the underlying service or good. In the instant matter, Plaintiffs explicitly allege that there is no comparable nexus between Google's interceptions and its ability to provide the electronic communication service at issue in this case, email. Specifically, in their Complaint, Plaintiffs state that Google's interceptions are "for [Google's] own benefit in other Google services unrelated to the service of email or the particular user." ECF No. 38-2 ¶ 97.

In light of the statutory text, case law, statutory scheme, and legislative history concerning the ordinary course of business exception, the Court finds that the section 2510(5)(a)(ii) exception is narrow and designed only to protect electronic communication service providers against a finding of liability under the Wiretap Act where the interception facilitated or was incidental to

provision of the electronic communication service at issue.[4] Plaintiffs have plausibly alleged that Google's reading of their emails was not within this narrow ordinary course of its business. Specifically, Plaintiffs allege that Google intercepts emails for the purposes of creating user profiles and delivering targeted advertising, which are not instrumental to Google's ability to transmit emails. The Consolidated Complaint alleges that "Google uses the content of the email messages [Google intercepts] and the derivative data it creates for its own benefit in other Google services unrelated to the service of email or the particular user." ECF No. 38-2 ¶¶ 97, 259(g). Plaintiffs support their assertion by suggesting that Google's interceptions of emails for targeting advertising and creating user profiles occurred independently from the rest of the email-delivery system. In fact, according to the Consolidated Complaint, the Gmail system has always had separate processes for spam filtering, antivirus protections, spell checking, language detection, and sorting than the devices that perform alleged interceptions that are challenged in this case. *Id.* ¶¶ 5, 200, 259(e). As such, the alleged interception of emails at issue here is both physically and purposively unrelated to Google's provision of email services. *Id.* ¶¶ 74, 259(g). Google's alleged interceptions are neither instrumental to the provision of email services, nor are they an incidental effect of providing these services. The Court therefore finds that Plaintiffs have plausibly alleged that the interceptions fall outside Google's ordinary course of business.

Furthermore, the D.C. Circuit has held in a section 2510(5)(a)(i) case that a defendant's actions may fall outside the "ordinary course of business" exception when the defendant violates its own internal policies. *See Berry*, 146 F.3d at 1010. In *Berry*, the court reversed a district court's grant of summary judgment in favor of the government on "ordinary course of business" grounds in part because the interception violated internal policies. That case concerned a Wiretap Act claim

[4] The Court does not find persuasive Google's slippery slope contention that a narrow interpretation of the ordinary course of business exception will make it impossible for electronic communication service providers to provide basic features, such as email searches or spam control. ECF No. 44 at 12–13. Some of these may fall within a narrow definition of "ordinary course of business" because they are instrumental to the provision of email service. Further, a service provider can seek consent to provide features beyond those linked to the provision of the service.

brought by a senior State Department officer against State Department Operations Center Watch Officers for monitoring the officer's phone call with another high-ranking officer. *Id.* at 1005. The D.C. Circuit noted that the "Operations Center Manual in effect at the time of these conversations cautioned that calls between Senior Department Officials . . . 'should not be monitored unless they so request.'" *Id.* at 1006. The court held that the "government's position [that this monitoring was within its ordinary course of business] is fatally undermined by the Operations Center guidelines which clearly indicate the norm of behavior the Watch Officers were to follow and which must be regarded as the ordinary course of business for the Center." *Id.* at 1009–10.

The Court finds that the reasoning of the D.C. Circuit applies equally in the section 2510(5)(a)(ii) context. Here, Plaintiffs allege that Google has violated its own policies and therefore is acting outside the ordinary course of business. Specifically, Plaintiffs allege that Google's Privacy Policies explicitly limit the information that Google may collect to an enumerated list of items, and that this list does not include content of emails. ECF No. 38-2 ¶¶ 187–91. Plaintiffs point to the language of the Privacy Policy that states that Google "may collect the following types of information" and then lists (1) information provided by the user (such as personal information submitted on the sign-up page), (2) information derived from cookies, (3) log information, (4) user communications to Google, (5) personal information provided by affiliated Google services and sites, (6) information from third party applications, (7) location data, and (8) unique application numbers from Google's toolbar. *Id.* ¶ 187; ECF No. 46-7. Plaintiffs further note that the updated Privacy Policy also stated that Google "collected information in two ways": "(1) information the user gives to Google—the user's personal information; and, (2) information Google obtains from the user's use of Google services, wherein Google lists: (a) the user's device information; (b) the user's log information; (c) the user's location information; (d) the user's unique application number; (e) information stored locally on the user's device; and, (e) [sic] information derived from cookies placed on a user's device." ECF No. 38-2 ¶ 189; ECF No. 46-10. Because content of emails between users or between users and non-users was not part of either

list, Plaintiffs allege that Google "violates the express limitations of its Privacy Policies." *Id.* ¶¶ 191, 195. The Court need not determine at this stage whether Plaintiffs will ultimately be able to prove that the Privacy Policies were intended to comprehensively list the information Google may collect. Rather, Plaintiffs' plausible allegations that the Privacy Policies were exhaustive are sufficient. Because Plaintiffs have alleged that Google exceeded the scope of its own Privacy Policy, the section 2510(5)(a)(ii) exception cannot apply.

Accordingly, the Court DENIES Google's Motion to Dismiss based on the section 2510(5)(a)(ii) exception.[5]

2. Consent

Google's second contention with respect to Plaintiffs' Wiretap Act claim is that all Plaintiffs consented to any interception of emails in question in the instant case. Specifically, Google contends that by agreeing to its Terms of Service and Privacy Policies, all Gmail users have consented to Google reading their emails. ECF No. 44 at 14–16. Google further suggests that even though non-Gmail users have not agreed to Google's Terms of Service or Privacy Policies, all non-Gmail users impliedly consent to Google's interception when non-Gmail users send an email to or receive an email from a Gmail user. *Id.* at 19–21.

If either party to a communication consents to its interception, then there is no violation of the Wiretap Act. 18 U.S.C. § 2511(2)(d).[6] Consent to an interception can be explicit or implied, but any consent must be actual. *See United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996);

[5] The Court notes that it is not the first court to reject Google's ordinary course of business exception theory on a motion to dismiss a challenge to the operation of Gmail. A federal district court in Texas ruled that it could not decide the question of ordinary course of business at the motion to dismiss phase. *See Dunbar v. Google, Inc.*, No. 10-CV-00194-MHS, ECF No. 61 (E.D. Tex. May 23, 2011). A state court in Massachusetts also rejected a similar claim under state law. *Marquis v. Google, Inc.*, No. 11-2808-BLSI (Mass Super. Ct. Jan. 17, 2012).

[6] However, to establish a consent defense under the state laws at issue in this case, both parties — the sender and the recipient of the communication — must consent to the alleged interception. *See* Fla. Stat. § 934.03(2)(d); Md. Code, Cts. & Jud. Proc. § 10-402(c)(3); 18 Pa. Cons. Stat. § 5704(4). Because the Court finds that no party has consented to any of the interceptions at issue in this case, the difference between the federal law's one-party consent regime and the state laws' two-party consent regimes is not relevant at this stage.

U.S. v. Amen, 831 F.2d 373, 378 (2d Cir. 1987); *U.S. v. Corona-Chavez*. 328 F.3d 974, 978 (8th Cir. 2003). Courts have cautioned that implied consent applies only in a narrow set of cases. *See Watkins*, 704 F.2d at 581 (holding that consent should not be "cavalierly implied"); *In re Pharmatak*, 329 F.3d at 20. The critical question with respect to implied consent is whether the parties whose communications were intercepted had adequate notice of the interception. *Berry*, 146 F.3d at 1011. That the person communicating knows that the interceptor has the *capacity* to monitor the communication is insufficient to establish implied consent. *Id*. Moreover, consent is not an all-or-nothing proposition. Rather, "[a] party may consent to the interception of only part of a communication or to the interception of only a subset of its communications." *In re Pharmatrack, Inc.*, 329 F.3d at 19.

In its Motion to Dismiss, Google marshals both explicit and implied theories of consent. Google contends that by agreeing to Google's Terms of Service and Privacy Policies, Plaintiffs who are Gmail users expressly consented to the interception of their emails. ECF No. 44 at 14–16. Google further contends that because of the way that email operates, even non-Gmail users knew that their emails would be intercepted, and accordingly that non-Gmail users impliedly consented to the interception. *Id.* at 19–20. Therefore, Google argues that in all communications, both parties — regardless of whether they are Gmail users — have consented to the reading of emails. *Id.* at 13–14. The Court rejects Google's contentions with respect to both explicit and implied consent. Rather, the Court finds that it cannot conclude that any party — Gmail users or non-Gmail users — has consented to Google's reading of email for the purposes of creating user profiles or providing targeted advertising.

Google points to its Terms of Service and Privacy Policies, to which all Gmail and Google Apps users agreed, to contend that these users explicitly consented to the interceptions at issue. The Court finds, however, that those policies did not explicitly notify Plaintiffs that Google would intercept users' emails for the purposes of creating user profiles or providing targeted advertising.

Section 8 of the Terms of Service that were in effect from April 16, 2007, to March 1, 2012, stated that "Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service."[7] ECF No. 46-5 at 4. This sentence was followed by a description of steps users could take to avoid sexual and objectionable material. *Id.* ("For some of the Services, Google may provide tools to filter out explicit sexual content."). Later, section 17 of the Terms of Service stated that "advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information." *Id.* at 8.

The Court finds that Gmail users' acceptance of these statements does not establish explicit consent. Section 8 of the Terms of Service suggests that content may be intercepted under a different set of circumstances for a different purpose — to exclude objectionable content, such as sexual material. This does not suggest to the user that Google would intercept emails for the purposes of creating user profiles or providing targeted advertising. *Watkins*, 704 F.2d at 582 ("[C]onsent within the meaning of section 2511(2)(d) is not necessarily an all or nothing proposition; it can be limited. It is the task of the trier of fact to determine the scope of the consent and to decide whether and to what extent the interception exceeded that consent."); *In re Pharmatrack, Inc.*, 329 F.3d at 19 ("Thus, a reviewing court must inquire into the dimensions of the consent and then ascertain whether the interception exceeded those boundaries.") (internal quotation marks omitted). Therefore, to the extent that section 8 of the Terms of Service establishes consent, it does so only for the purpose of interceptions to eliminate objectionable content. The Consolidated Complaint suggests, however, that Gmail's interceptions for the purposes of targeted advertising and creation of user profiles was separate from screening for any objectionable content. *See* ECF No. 38-2 ¶¶ 5, 200. Because the two processes were allegedly separate, consent to one does not equate to consent to the other.

[7] It is undisputed that the term "Service" throughout Google's Terms of Service includes Gmail.

Section 17 of the Terms of Service — which states that Google's "advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information" — is defective in demonstrating consent for a different reason: it demonstrates only that Google has the *capacity* to intercept communications, not that it will. *Berry*, 146 F.3d at 1011 (holding that knowledge of defendant's capacity to monitor is insufficient to establish consent). Moreover, the language suggests only that Google's advertisements were based on information "stored on the Services" or "queries made through the Services" — not information in transit via email. Plaintiffs here allege that Google violates the Wiretap Act, which explicitly protects communications in transit, as distinguished from communications that are stored. Furthermore, providing targeted advertising is only one of the alleged reasons for the interceptions at issue in this case. Plaintiffs also allege that Google intercepted emails for the purposes of creating user profiles. *See* ECF No. 38-2 ¶ 95. Section 17, to the extent that it suggests interceptions, only does so for the purposes of providing advertising, not creating user profiles. Accordingly, the Court finds that neither section of the Terms of Service establishes consent.

The Privacy Policies in effect from August 8, 2008, to October 3, 2010, to which all Gmail users agreed and upon which Google now relies, do not clarify Google's role in intercepting communications between its users. The Policies stated that Google may collect "[i]nformation you provide, [c]ookies[,] [l]og information[,] [u]ser communications to Google[,] [a]ffiliated sites, [l]inks[,] [and] [o]ther sites." *See* ECF No. 46-7 at 2–3. Google described that it used such information for the purposes of "[p]roviding our services to users, including the display of customized content and advertising." *Id.* at 3. In 2010, Google later updated the Policy to state that the collected information would be used to "[p]rovide, maintain, protect, and improve our services (including advertising services) and develop new services." *See* ECF No. 46-9 at 3. Nothing in the Policies suggests that Google intercepts email communication in transit between users, and in fact, the policies obscure Google's intent to engage in such interceptions. The Privacy Policies explicitly state that Google collects "user communications . . . *to Google*." *See*

ECF No. 46-7 at 3 (emphasis added). This could mislead users into believing that user communications to each other or to nonusers were not intercepted and used to target advertising or create user profiles. As such, these Privacy Policies do not demonstrate explicit consent, and in fact suggest the opposite.

After March 1, 2012, Google modified its Terms of Service and Privacy Policy. The new policies are no clearer than their predecessors in establishing consent. The relevant part of the new Terms of Service state that when users upload content to Google, they "give Google (and those [Google] work[s] with) a worldwide license to use . . ., create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), . . . and distribute such content." *See* ECF No. 46-6 at 3. The Terms of Service cite the new Privacy Policy, in which Google states to users that Google "may collect information about the services that you use and how you use them, like when you visit a website that uses our advertising services or you view and interact with our ads and content. This information includes: [d]evice information[,] [l]og information[,] [l]ocation information[,] [u]nique application numbers[,] [l]ocal storage[,] [c]ookies[,] and anonymous identifiers." ECF No. 46-10 at 3. The Privacy Policy further states that Google "use[s] the information [it] collect[s] from all [its] services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and [its] users. [Google] also use[s] this information to offer you tailored content — like giving you more relevant search results and ads." *See* ECF No. 46-10 at 3. These new policies do not specifically mention the content of users' emails to each other or to or from non-users; these new policies are not broad enough to encompass such interceptions. Furthermore, the policies do not put users on notice that their emails are intercepted to create user profiles. The Court therefore finds that a reasonable Gmail user who read the Privacy Policies would not have necessarily understood that her emails were being intercepted to create user profiles or to provide targeted advertisements. Accordingly, the Court finds that it cannot conclude at this phase that the new policies demonstrate that Gmail user Plaintiffs consented to the interceptions.

Finally, Google contends that non-Gmail users — email users who do not have a Gmail account and who did not accept Gmail's Terms of Service or Privacy Policies — nevertheless impliedly consented to Google's interception of their emails to and from Gmail users, and to Google's use of such emails to create user profiles and to provide targeted advertising. ECF No. 44 at 19–20. Google's theory is that all email users understand and accept the fact that email is automatically processed. *Id.* However, the cases Google cites for this far-reaching proposition hold only that the sender of an email consents to the intended recipients' recording of the email — not, as has been alleged here, interception by a third-party service provider. *See State v. Townsend*, 57 P.3d 255, 260 (Wash. 2002) (finding consent and therefore no violation of Washington's privacy act when email and instant message communications sent to an undercover police officer were used against criminal defendant); *State v. Lott*, 879 A.2d 1167, 1172 (N.H. 2005) (same under New Hampshire law); *Commonwealth v. Proetto*, 771 A.2d 823, 829 (Pa. Super. Ct. 2001) (holding that the Pennsylvania anti-wiretapping law was not violated when the recipient forwarded emails and chat messages to the police). Google has cited no case that stands for the proposition that users who send emails impliedly consent to interceptions and use of their communications by third parties other than the intended recipient of the email. Nor has Google cited anything that suggests that by doing nothing more than receiving emails from a Gmail user, non-Gmail users have consented to the interception of those communications. Accepting Google's theory of implied consent — that by merely sending emails to or receiving emails from a Gmail user, a non-Gmail user has consented to Google's interception of such emails for any purposes — would eviscerate the rule against interception. *See Watkins*, 704 F.2d at 581 ("It would thwart th[e] policy [of protecting privacy] if consent could routinely be implied from circumstances.").[8] The Court does

[8] In their briefs, the parties dispute whether members of the putative class of Gmail users who are minors consented to the interceptions. Google contends that minors are bound by the Terms of Service and Privacy Policies. ECF No. 44 at 16–17. Google argues that the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–08, preempts any state law that would have rendered the minors' consent ineffective. The Court need not reach the issue of whether minors are bound by the Terms of Service or the Privacy Policies because the Court concludes that even if the minors

not find that non-Gmail users who are not subject to Google's Privacy Policies or Terms of Service have impliedly consented to Google's interception of their emails to Gmail users.

Because Plaintiffs have adequately alleged that they have not explicitly or implicitly consented to Google's interceptions, the Court DENIES Google's Motion to Dismiss on the basis of consent.[9]

B. CIPA

CIPA, Cal. Penal Code § 630, *et seq.*, California's anti-wiretapping and anti-eavesdropping statute, prohibits unauthorized interceptions of communications in order "to protect the right of privacy." Cal. Penal Code § 630. The California Legislature enacted CIPA in 1967 in response to "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications." *Id.*

Section 631 prohibits wiretapping or "any other unauthorized connection" with a "wire, line, cable, or instrument." *See* Cal. Penal Code § 631(a). The California Supreme Court has held that section 631 protects against three distinct types of harms: "intentional wiretapping, willfully attempting to learn the contents or meaning of a communication in transit over a wire, and attempting to use or communicate information obtained as a result of engaging in either of the previous two activities." *Tavernetti v. Superior Court*, 583 P.2d 737, 741 (Cal. 1978). Section 632 prohibits unauthorized electronic eavesdropping on confidential conversations. *See* Cal. Penal Code § 632(a). To state a claim under section 632, a plaintiff must allege an electronic recording

---

are subject to these agreements, the agreements did not establish consent. Similarly, Google contends that Google Apps users are also bound by the Terms of Service and Privacy Policies even though they were required by their educational institutions or ISPs to use Gmail. ECF No. 44 at 17–18. Again, because the Court concludes that the agreements did not establish consent, the Court need not reach the issue of whether Google Apps users are bound by the agreements.

[9] Other courts have also rejected Google's consent defense against state and federal anti-wiretapping challenges to the operation of Gmail. *See Dunbar v. Google, Inc.*, No. 10-cv-00194-MHS, ECF No. 61 (E.D. Tex. May 23, 2011); *Marquis v. Google, Inc.*, No. 11-2808-BLSI (Mass Super. Ct. Jan. 17, 2012).

of or eavesdropping on a confidential communication, and that not all parties consented to the eavesdropping. *Flanagan v. Flanagan*, 41 P.3d 575, 577 (Cal. 2002).

CIPA also contains a public utility exemption, which applies to claims under both sections 631 and 632. Cal. Penal Code §§ 631(b), 632(e). Neither section applies "to any public utility engaged in the business of providing communications services and facilities, or to the officers, employees, or agents thereof, where the acts otherwise prohibited by this section are for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility." Cal. Penal Code §§ 631(b), 632(e).

Plaintiffs allege violations of both section 631 and section 632. *See* ECF No. 38-2 ¶ 321. Google moves to dismiss on five bases. *See* ECF No. 44 at 23–24, 27–28. Google contends that Plaintiffs lack standing to allege such violations and that the California law should not apply due to choice of law principles. *See id*. Google also moves to dismiss Plaintiffs' claims on substantive bases, contending that neither section 631 nor section 632 applies to email and that the public utility exemption applies. *See* ECF No. 44 at 21–23, ECF No. 56 at 14–15. Finally, Google moves to dismiss Plaintiffs' section 632 claim because the communications at issue in this case were not confidential as defined by that section and because that section is preempted by the ECPA. *See* ECF No. 44 at 25–27.

1. Standing

Google first contends that Plaintiffs lack standing under Article III to assert a CIPA claim. A federal court must ask whether a plaintiff has suffered sufficient injury to satisfy the "case or controversy" requirement of Article III of the U.S. Constitution. ECF No. 44 at 23–24. To satisfy Article III standing, a plaintiff must allege: (1) injury-in-fact that is concrete and particularized, as well as actual or imminent; (2) wherein injury is fairly traceable to the challenged action of the defendant; and (3) it is likely (not merely speculative) that injury will be redressed by a favorable decision. *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180–81 (2000); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992). A suit brought by a plaintiff

without Article III standing is not a "case or controversy," and an Article III federal court therefore lacks subject matter jurisdiction over the suit.

Google's contention is that Plaintiffs have not suffered the "injury" required by Article III to confer standing. ECF No. 44 at 24. Under Ninth Circuit precedent, the injury required by Article III may exist by virtue of "statutes creating legal rights, the invasion of which creates standing." *See Edwards v. First Am. Fin. Corp.*, 610 F.3d 514, 517 (9th Cir. 2010) (quoting *Warth v. Seldin*, 422 U.S. 490, 500 (1975)). In such cases, the "standing question . . . is whether the constitutional or statutory provision on which the claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief." *Id.* (quoting *Warth*, 422 U.S. at 500). In *Edwards*, the Ninth Circuit has held that the Real Estate Settlement Procedures Act ("RESPA") conferred standing to a homeowner who sought to challenge the kickback relationship between the title insurer and title agency despite the fact that the homeowner suffered no independent injury, through, for example, overpayment. *Id.* The court there held that the structure of RESPA was such that independent injury was not needed; a plaintiff's showing that the defendant's conduct violated the statute was sufficient to confer standing. *Id.* [10]

Applying the Ninth Circuit's decision in *Edwards*, courts in this district have found that allegations of a Wiretap Act violation are sufficient to establish standing. In *In re Facebook Privacy Litigation*, 791 F. Supp. 2d 705, 712 (N.D. Cal. 2011), for example, the court held that the "Wiretap Act provides that any person whose electronic communication is 'intercepted, disclosed, or intentionally used' in violation of the Act may in a civil action recover from the entity which engaged in that violation." Accordingly, the court found that where the plaintiffs had alleged that

[10] The United States Supreme Court granted a petition for a writ of certiorari in *Edwards* on the question of whether statutory injury alone could confer standing under Article III even though the Courts of Appeal that had considered the question had unanimously concluded that allegations of RESPA violations alone sufficed for standing. *See First Am. Fin. Corp. v. Edwards*, 131 S. Ct. 3022 (2011). After oral argument, however, the Supreme Court dismissed the writ as improvidently granted. *See First Am. Fin. Corp. v. Edwards*, 132 S. Ct. 2536 (2012). This left in place the Ninth Circuit's decision in *Edwards*, which remains binding authority that this Court must apply, as it does here.

their communications had been intercepted, they "alleged facts sufficient to establish that they have suffered the injury required for standing under Article III." *Id.* at 712; *see also In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1055 (N.D. Cal. 2012) ("[A] violation of the Wiretap Act . . . may serve as a concrete injury for the purposes of Article III injury analysis."); *In re Google, Inc. Privacy Policy Litig.*, 2012 WL 6738343 (N.D. Cal. Dec. 28, 2012) ("[If viable], Plaintiffs' Wiretap Act claim might help [show standing], [because] a violation of the rights provided under the statute may be sufficient by itself to confer standing.")

The reasoning of these cases that find standing when there is an allegation of a Wiretap Act violation applies equally to CIPA. Like the Wiretap Act, CIPA creates a private right of action when a defendant engages in wiretapping or eavesdropping. *Compare* 18 U.S.C. § 2520(a) ("[A]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation), *with* Cal. Penal Code § 637.2(a) ("Any person who has been injured by a violation of this chapter may bring an action against the person who committed the violation."). Further, like the Wiretap Act, CIPA authorizes an award of statutory damages any time a defendant violates the provisions of the statute without any need to show actual damages. *Compare* 18 U.S.C. § 2520(c) (authorizing statutory damages), *with* Cal. Penal Code § 637.2(a)(1) (same) *and* Cal. Penal Code § 637.2(c) ("It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."). Therefore, the Court finds that the allegation of a violation of CIPA, like an allegation of the violation of the Wiretap Act, is sufficient to confer standing without any independent allegation of injury. Like both RESPA and the Wiretap Act, therefore, CIPA creates a statutory right the violation of which confers standing on a plaintiff.

Google relies exclusively on the differences in statutory text between CIPA and the Wiretap Act to contend that CIPA requires an independent allegation of injury even where the Wiretap Act does not. Specifically, Google notes that the provision of CIPA that creates a cause of action states

that, "[a]ny person who *has been injured* by a violation of this chapter may bring an action against the person who committed the violation." Cal. Penal Code § 637.2(a) (emphasis added). Google's contention is that the word "injured" means that Plaintiffs must show some injury independent of the invasion of their statutory rights under CIPA. Google cites no authority for the proposition that section 637.2 requires independent injury or the proposition that the word "injured" triggers an obligation to demonstrate independent injury for the purposes of Article III standing. The California case law on CIPA cuts against Google's contention that "injured" requires independent injury. As the California Court of Appeals has stated, "Section 637.2 is fairly read as establishing that no violation of the Privacy Act [CIPA] is to go unpunished. Any invasion of privacy involves an affront to human dignity which the Legislature could conclude is worth at least $3,000. The right to recover this statutory minimum accrued at the moment the Privacy Act [CIPA] was violated." *Friddle v. Epstein*, 21 Cal. Rptr. 85, 92 (Cal Ct. App. 1993); *see also id.* ("Plaintiff invaded defendants' privacy and violated the Privacy Act [CIPA] at the moment he began making his secret recording. No subsequent action or inaction is of consequence to this conclusion."); *accord Ribas v. Clark*, 38 Cal. 3d 355, 365 (Cal. 1985) ("In view of the manifest legislative purpose to accord every citizen's privacy the utmost sanctity, section 637.2 was intended to provide those who suffer an infringement of this aspect of their personal liberty a means of vindicating their right.").

Accordingly, the Court finds that CIPA and the Wiretap Act are not distinguishable for the purposes of standing. Because courts have, under existing Ninth Circuit authority, consistently held that the invasion of rights under the Wiretap Act is sufficient for Article III standing, this Court concludes that the same is true of CIPA. All Plaintiffs need allege is an invasion of statutory CIPA rights to survive a motion to dismiss on standing grounds. There is no dispute that they have done so here. The Court therefore DENIES Google's Motion to Dismiss the CIPA claims on standing grounds.

2. Choice of Law

Google contends that under choice of law principles, California law should not apply and that the Court should accordingly dismiss Plaintiffs' California claims. ECF No. 44 at 27–30. Plaintiffs contend that the choice of law analysis should wait for later stages of the proceedings. ECF No. 53 at 28. As set forth below, the choice of law inquiry raises complicated, fact-intensive questions better answered at later stages of the litigation. Therefore, the Court DENIES the Motion to Dismiss on choice of law grounds.

To determine which state's law should apply, "[a] federal court . . . must look to the forum state's choice of law rules to determine the controlling substantive law." *Mazza v. American Honda Motor Co., Inc.*, 666 F.3d 581, 589 (9th Cir. 2012) (internal quotation marks omitted). Under California law, class action plaintiffs have the burden to "show that California has sufficient contact or sufficient aggregation of contacts to the claims of each class member." *Id*. at 589–90 (internal quotation marks omitted). If this showing is made, "the burden shifts to the other side to demonstrate that foreign law, rather than California law, should apply to class claims." *Id*. at 590.

"California courts apply the so-called governmental interest analysis" to determine whether California law should be applied on a class-wide basis." *Kearney v. Salomon Smith Barney, Inc.*, 137 P.3d 914, 917 (Cal. 2006). Under this three-part test: "[1] the court determines whether the relevant law of each of the potentially affected jurisdictions with regard to the particular issue in question is the same or different . . .[; 2] if there is a difference, the court examines each jurisdiction's interest in the application of its own law under the circumstances of the particular case to determine whether a true conflict exists . . . [; and 3] if the court finds there is a true conflict, it carefully evaluates and compares the nature and strength of the interest of each jurisdiction in the application of its own law . . . and then ultimately applies the law of the state whose interest would be more impaired if its law were not applied." *Mazza*, 666 F.3d at 590 (quoting *McCann v. Foster Wheeler, LLC*, 225 P.3d 517, 527 (Cal. 2010)).

The Court finds that Plaintiffs have established that their claims are sufficiently related to California to trigger application of the three-part test. The Ninth Circuit has held that sufficient aggregate contacts with California are established in a class action when a defendant's corporate headquarters is located in the state, advertising materials pertaining to representations the company made to class members are created in the state, and one fifth of the class is located in California. *Mazza*, 666 F.3d at 590. In this case, as Plaintiffs allege, Google is located in California, it developed and implemented the practices at issue in this action in California, and one or more of the physical interceptions at the heart of Plaintiffs' claims occurred in California. ECF No. 38-2 ¶ 290 ("Google's acts in violation of CIPA occurred in the State of California . . . . Google's implementation of its business decisions, practices, and standard ongoing policies which violate CIPA took place in the State of California. Google profited in the State of California"); ECF No. 53 at 29. In short, California is the epicenter of the practices at issue in this case for all Plaintiffs. Therefore, the Court finds that Plaintiffs have shown that "California has a constitutionally sufficient aggregation of contacts to the claims of each putative class member." *Mazza*, 666 F.3d at 590.

Because the Court finds sufficient aggregate contacts, it turns to the first of the three-part inquiry to determine whether California law or the law of another state should apply to the class claims. The Court must determine whether there is a material conflict between the laws of California and those of the Plaintiffs' home states. Google contends that there is a conflict because Alabama and Maryland law are narrower with respect to scope of liability, enforcement mechanisms, and available remedies. ECF No. 44 at 28.

The Court cannot, at this stage, determine whether there are differences with respect to the scope of liability. Google correctly contends that under Alabama and Maryland's law, one party's consent is sufficient to negate an interception, while under California law, both parties must consent. *Id.* Yet, it is not clear whether this difference in the scope of liability is material, that is whether, it "make[s] a difference in this litigation." *Mazza*, 666 F.3d at 590. This is because

Plaintiffs contend that neither party has consented, while Google contends that all parties have consented. ECF No. 38-2 ¶ 102–97, ECF No. 44 at 13–14. Accordingly, on either party's theory of liability, the difference in state law with respect to the consent standard would not be a material difference.

Therefore, the Court finds that it cannot conduct a meaningful choice of law analysis, such as that contemplated by *Mazza*, at this early stage of the litigation where the issues of contention are still in flux.[11] As other courts have noted, the rigorous choice of law analysis required by *Mazza* cannot be conducted at the motion to dismiss stage. *See Clancy v. The Bromley Tea Co.*, 2013 WL 4081632 (N.D. Cal. Aug. 9, 2013) ("Such a detailed choice-of-law analysis is not appropriate at [the motion for judgment on the pleadings] stage of the litigation. Rather, such a fact-heavy inquiry should occur during the class certification stage, after discovery."); *In re Clorox Consumer Litig.*, 894 F. Supp. 2d 1224, 1237 (N.D. Cal. 2012) ("Significantly, *Mazza* was decided on a motion for class certification, not a motion to strike. At [the motion to dismiss] stage of the instant litigation, a detailed choice-of-law analysis would be inappropriate. Since the parties have yet to develop a factual record, it is unclear whether applying different state consumer protection statutes could have a material impact on the viability of Plaintiffs' claims.") (citation omitted); *Donohue v. Apple, Inc.*, 871 F. Supp. 2d 913, 923 (N.D. Cal. 2012) ("Although *Mazza* may influence the decision whether to certify the proposed class and subclass, such a determination is premature. At [the motion to dismiss] stage in the litigation—before the parties have submitted briefing regarding either choice-of-law or class certification—plaintiff is permitted to assert claims under the laws of different states in the alternative."); *In re Sony Grand Wega KDF-E A10/A20 Series Rear Projection HDTV Television Litig.*, 758 F. Supp. 2d 1077, 1096 (S.D. Cal. 2010) ("In a

[11] The Court recognizes that additional conflicts may arise out of California's acknowledgement of a private right of action and/or the remedies California allows under CIPA. However, under California choice of law analysis, differences in remedies alone are not dispositive. The Court may resolve the conflict between California and foreign law by "apply[ing] California law in a restrained manner" with regard to monetary damages. *Kearney*, 39 Cal. 4th at 100–01. In any case, the Court will resolve all conflict of law questions at the class certification stage.

putative class action, the Court will not conduct a detailed choice-of-law analysis during the pleading stage.").

Accordingly, the Court defers resolution of the choice of law issues until the class certification phase and DENIES Google's Motion to Dismiss on the basis of choice of law without prejudice to Google raising this argument at a later stage.

3. Section 631

Google contends that even if Plaintiffs' section 631 challenge is not procedurally barred, it is substantively deficient because that section does not apply to emails. ECF No. 44 at 21–23. Further, in its reply brief, Google contends that the public utility exemption applies. ECF No. 56 at 14–15.

a. Application to Email

The Court finds that there is no binding authority with respect to whether section 631 applies to email.[12] The only authority from the California courts is a Superior Court ruling. *See Diamond v. Google, Inc.*, CIV-1202715 (Cal. Super. Ct., Marin Cnty. Aug. 14, 2013) (finding, without providing analysis, that allegations of interception of email communication are sufficient to state a claim under Cal. Penal Code § 631). While two federal courts have been confronted with the application of CIPA to Internet browsing history and emails, those matters were resolved on other grounds before reaching the question of CIPA's application to digital technologies generally or email specifically. *Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022 (N.D. Cal. 2011); *Bradley v. Google*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006).

In the absence of binding authority, this Court must predict what the California Supreme Court would do if confronted with this issue. *See Valentine*, 804 F. Supp. 2d at 1027. The Court begins by looking to the text. Section 631 establishes liability for:

[12] California courts have, however, applied section 632 to internet communication technologies. *See People v. Nakai*, 183 Cal. App. 4th 499 (2010); *People v. Cho*, 2010 WL 4380113 (Cal. Ct. App. Nov. 5, 2010); *People v. Griffitt*, 2010 WL 5006815 (Cal. Ct. App. Dec. 9, 2010).

> [a]ny person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraphic or telephone wire, line cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully or without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable, or is being sent from, or received at any place within this state.

Cal. Penal Code § 631. Google contends that the language "reads or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable" applies only to interception of content on *telephone and telegraphic* wires, lines, or cables, as the first clause of the statute describes. ECF No. 44 at 21. As a result, Google contends that the second clause, upon which Plaintiffs rely, cannot apply to email since emails are not messages, reports or communications that pass over telephone or telegraphic wires. *Id.*

The Court rejects Google's reading of the statute. As a threshold matter, the second clause of the statute, which creates liability for individuals who "read[] or attempt[] to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over *any* wire, line or cable, or is being sent from, or received at any place within this state[,]" is not limited to communications passing over "telegraphic or telephone" wires, lines, or cables. *See* Cal. Penal Code § 631 (emphasis added). Furthermore, the Court finds no reason to conclude that the limitation of "telegraphic or telephone" on "wire, line, cable, or instrument" in the first clause of the statute should be imported to the second clause of the statute. The second clause applies only to "wire[s], line[s], or cable[s]" — not "instrument[s,]" which are included in the first clause. The Court finds that this difference in coverage between the first and second clauses suggests that the Legislature intended the two clauses to apply to different types of communications. Accordingly, the Court rejects Google's contention that the limitations in the first clause must also apply to the second clause. The Court therefore finds that the plain language of the statute is broad enough to encompass email.

Further, the California Supreme Court's repeated finding that the California legislature intended for CIPA to establish broad privacy protections supports an expansive reading of the statute. *See Flanagan*, 41 P.3d at 581 ("In enacting [CIPA], the Legislature declared in broad terms its intent to protect the right of privacy of the people of this state from what it perceived as a serious threat to the free exercise of personal liberties. This philosophy appears to lie at the heart of virtually all the decisions construing [CIPA]."") (internal quotation marks and citations omitted); *Ribas v. Clark*, 696 P.2d 637, 641 (Cal. 1985) (finding it is "probable" that the legislature designed Section 631 as a catch all to "proscrib[e] attempts to circumvent other aspects of the Privacy Act, e.g., by requesting a secretary to secretly transcribe a conversation over an extension, rather than tape recording it in violation of section 632"); *Tavernetti v. Superior Court*, 583 P.2d 737, 742 (Cal. 1978) ("Th[e] forceful expression of the constitutional stature of privacy rights [in California] reflects a concern previously evinced by the Legislature in enacting the invasion of privacy provisions of the Penal Code.").

Moreover, the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme. For example, in a previous evolution in communications technology, the California Supreme Court interpreted "telegraph" functionally, based on the type of communication it enabled. In *Davis v. Pacific Telephone & Telegraph*, the Supreme Court held that "*telegraph* lines" in a criminal law proscribing the cutting of lines included *telephone* lines because "[t]he idea conveyed by each term is the sending of intelligence to a distance . . . [thus] the term 'telegraph' means any apparatus for transmitting messages by means of electric currents and signals." *Davis v. Pacific Telephone & Telegraph Co.*, 59 P. 698, 699 (Cal. 1899); *see also Apple v. Superior Court*, 292 P.2d 883, 887 (Cal. 2013) ("Fidelity to legislative intent does not make it impossible to apply a legal text to technologies that did not exist when the text was created." (internal quotation marks omitted)).

In line with the plain language of the statute, the California Supreme Court's pronouncements regarding the broad legislative intent underlying CIPA to protect privacy, and the

California courts' approach to updating obsolete statutes in light of emerging technologies, the Court finds that section 631 of CIPA applies to emails.

b. Public Utility Exemption

Google contends that even if CIPA applies to emails, it is a "public utility" that is exempt from the statute. ECF No. 56 at 14–15. The Court declines to reach this conclusion. California's Constitution defines "public utilities" as "[p]rivate corporations and persons that own, operate, control, or manage a line, plant, or system for . . . the transmission of telephone and telegraph messages . . . directly or indirectly to or for the public." Cal. Const., art. XII, § 3. The California Public Utility Code further defines this definition of "public utility" as "every common carrier . . . , telephone corporation [or] telegraph corporation . . ., where the service is performed for, or the commodity is delivered to, the public or any portion thereof." Cal. Pub. Util. Code § 216(a). The Public Utility Code further specifies that a "telegraph corporation" is "every corporation or person *owning, controlling, operating, or managing* any telegraph line for compensation within this State." *Id.* § 236 (emphasis added). "Telegraph line" is defined as "all conduits, ducts, poles, wires, cables, instruments, and appliances, and all other real estate, fixtures, and personal property owned, controlled, operated, or managed in connection with or to facilitate communication by telegraph, whether such communication is had with or without the use of transmission wires." *Id.* § 235. The code uses analogous definitions for "telephone corporations" and "telephone lines." *Id.* §§ 233, 234.

In short, in California, a "public utility" is a precisely defined entity subject to an expansive and exacting regulatory regime. Under the plain language of the statutes, merely operating a service over a telephone or telegraph line does not render a company a public utility. Rather, the critical question is whether the company owns, controls, operates or manages a telephone or telegraph line. Cal. Pub. Util. Code § 236. Nothing in the record suggests that Google owns, controls, operates, or manages a telephone or telegraph lines in California. Accordingly, the Court finds that Google is not a "public utility" and thus does not qualify for the public utility exemption

of Cal. Penal Code §§ 631(b). The Court therefore DENIES Google's Motion to Dismiss Plaintiffs' section 631 claims.

4. Section 632

To state a claim under California Penal Code § 632, a plaintiff must prove (1) an electronic recording of or eavesdropping on (2) a "confidential communication" (3) to which all parties did not consent. *Flanagan*, 41 P.3d at 577. As set forth below, Plaintiffs have not established that the communications at issue are confidential pursuant to section 632. Accordingly, the Court GRANTS without prejudice Google's Motion to Dismiss Plaintiffs' section 632 claim. Because this second element of a section 632 claim is not met, the Court need not address whether email constitutes an electronic recording under the statute nor need it address whether there was consent under California law.[13]

A conversation is "confidential" under section 632 "if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded . . . . The standard of confidentiality is an objective one defined in terms of reasonableness." *Faulkner v. ADT Sec. Servs., Inc.*, 706 F.3d 1017, 1019 (9th Cir. 2013). "To prevail against a 12(b)(6) motion, then, [the plaintiff] would have to allege facts that would lead to the plausible inference that his was a confidential communication — that is, a communication that he had an objectively reasonable expectation was not being recorded." *Id.* at 1020.

There is no authority from the California courts addressing whether emails can be confidential communication. Some decisions from the California appellate courts, however, suggest that internet-based communication cannot be confidential. These courts rely on the theory that individuals cannot have a reasonable expectation that their online communications will not be recorded. In *People v. Nakai*, 107 Cal. Rptr. 3d 402 (Cal. Ct. App. 2010), for example, the California Court of Appeals found that section 632 did not protect instant message communications

[13] The Court also need not address whether the ECPA preempts section 632 of CIPA, as Google contends. *See* ECF No. 44 at 26–27.

of a criminal defendant charged with attempting to send harmful matter to a minor with intent to arouse and seduce. There, the defendant, an adult man, had sent sexually explicit material via instant message to a 35-year-old decoy, who was posing as a 12-year-old girl. *Id.* at 405–07. The appellate court found that while the defendant intended that the communication be kept confidential between himself and the recipient, he could not reasonably expect that the communications would not be recorded. *Id.* at 418. Specifically, the court found that the fact that the intended recipient could easily forward the information to others militated against finding that there was a reasonable expectation that the instant message would be kept confidential. *Id.* As the court stated, "it was not reasonable for defendant to expect the communications to be confidential because the circumstances reflect that the communications could have easily been shared or viewed by . . . any computer user with whom [the intended recipient] wanted to share the communication." *Id.*; *see also People v. Cho*, 2010 WL 4380113 (Cal. Ct. App. Nov. 5, 2010) (holding chat conversations are not confidential under section 632); *People v. Griffitt*, 2010 WL 5006815 (Cal. Ct. App. Dec. 9, 2010) ("Everyone who uses a computer knows that the recipient of e-mails and participants in chat rooms can print the e-mails and chat logs and share them with whoever they please, forward them or otherwise send them to others.").

The Court finds that Plaintiffs have not alleged facts that lead to the plausible inference that the communication was not being recorded because email by its very nature is more similar to internet chats. Unlike phone conversations, email services are by their very nature recorded on the computer of at least the recipient, who may then easily transmit the communication to anyone else who has access to the internet or print the communications. Thus, Plaintiffs have not plausibly alleged that they had an objectively reasonable expectation that their email communications were "confidential" under the terms of section 632.[14]

[14] The Court's holding that the emails are not "confidential" under section 632 is consistent with the conclusion that Plaintiffs have nevertheless not consented to Google's interceptions under the Wiretap Act and state analogues. *See supra* section III.A.2. Determining whether a communication is confidential under section 632 requires the Court to look to whether the intended

Therefore, the Court GRANTS Google's Motion to Dismiss Plaintiffs' section 632 claims. In a case concerning whether a communication was confidential under section 632, the Ninth Circuit affirmed a district court's grant of a defendant's motion to dismiss, but "[i]n an abundance — perhaps an overabundance — of caution" remanded "to the district court for it to consider allowing the plaintiff to amend his complaint in a manner that would satisfy federal pleading standards." *Faulkner*, 706 F.3d at 1021. Here too this Court in "an abundance of caution" grants Plaintiffs' leave to amend their Consolidated Complaint. *Id.*; Fed. R. Civ. Proc. 15(a).

C. Other State Law Claims

Plaintiffs also allege that Google violated Pennsylvania, Maryland, and Florida law. With respect to Maryland and Florida law, Google's sole contention in its Motion to Dismiss is that these claims are derivative of Plaintiffs' federal causes of action. *See* ECF No. 44 at 5. Google expressly acknowledges that the Maryland and Florida anti-wiretapping statutes mirror the ECPA. *See id.* Therefore, Google's Motion to Dismiss these claims is based on its Motion to Dismiss Plaintiffs' federal claims. Because the Court denies Google's Motion to Dismiss Plaintiffs' federal causes of action, the Court also DENIES Google's Motion to Dismiss Plaintiffs' Maryland and Florida claims.

Google offers an independent basis for dismissing part of Plaintiff's Pennsylvania law cause of action. Specifically, Google contends that Pennsylvania law protects only the sender of communication from wiretapping, not the recipient of that communication. *See* ECF No. 44 at 13. As a result, Google moves to dismiss Plaintiffs' Pennsylvania law claim brought by those who received emails from Gmail addresses. *Id.*

---

recipient of the communication is likely to share the communication. In contrast, the question of consent turns on whether Plaintiffs have authorized the third-party interceptor's interference in the communication. In the instant matter, the Court concludes that emails are not likely to be kept confidential by the intended recipients under section 632. Nevertheless, individuals do not consent to third parties' interception of their emails.

Google relies on *Klump v. Nazareth Area Sch. Dist.*, 425 F. Supp. 2d 622, 633 (E.D. Pa. 2006), where the court held that "[a] claimant must demonstrate 'that he engaged in [a] communication'. The intended recipient of an intercepted communication, therefore, has no standing to raise claim [sic] under section 5725." *See* ECF No. 44 at 13. Plaintiffs do not contest that *Klump* limits the scope of their Pennsylvania cause of action to those who sent emails to Gmail recipients and eliminates their cause of action against those who received emails from Gmail senders. Rather, Plaintiffs contend only that this Court should not follow *Klump* because that case was wrongly decided. *See* ECF No. 53 at 11. However, Plaintiffs do not point to any authority from the state or federal courts in Pennsylvania that is contrary to the court's holding in *Klump*. In the absence of contrary authority, this Court will follow the decision in *Klump*. Accordingly, the Court GRANTS Google's Motion to Dismiss with respect to the claims under Pennsylvania law raised by Plaintiffs who received emails from Gmail users. In an abundance of caution, however, the Court grants Plaintiffs leave to amend the Consolidated Complaint.

V. CONCLUSION

For the foregoing reasons, the Court hereby GRANTS Google's Motion to Dismiss with leave to amend with respect to Plaintiffs' CIPA section 632 claims and Plaintiffs' Pennsylvania law claim as it relates those who received emails from Gmail users. The Court DENIES Google's Motion to Dismiss with respect to all other claims. Plaintiffs shall file any amended complaint within 21 days of this order. Plaintiffs may not add new causes of action or parties without a stipulation or order of the Court under Rule 15 of the Federal Rules of Civil Procedure. Failure to cure deficiencies will result in dismissal with prejudice.

IT IS SO ORDERED.

Dated: September 26, 2013

Lucy H. Koh

LUCY H. KOH
United States District Judge